

Disclaimer

Legal disclaimer

This guide and its contents (the "Guide") are provided by NXGEN. All rights to the Guide and to the intellectual property embodied in it — including, without limitation, trademarks, trade names, logos and similar marks appearing in or on it — are protected by law. All right, title and interest in the Guide and in any related intellectual property rights belong to and remain with NXGEN and its licensors.

The Guide is provided free of charge, "as is" and for informational purposes only, without warranty of any kind. It is neither intended nor suitable to establish any legal relationship between the reader and NXGEN or its affiliates, including, without limitation, any obligation of NXGEN or its affiliates toward the reader.

The obligations of NXGEN and its affiliates in respect of NXGEN products or services purchased by a customer are governed exclusively by the terms of the agreement under which those products or services were purchased.

For clarification

The reader bears the entire risk as to the use, results and performance of the Guide. To the fullest extent permitted by applicable law, NXGEN disclaims and excludes all warranties, whether statutory, express or implied — including, without limitation, implied warranties of merchantability, fitness for a particular purpose, title and non-infringement of third-party rights — as well as any liability or warranty arising from suggestions, specifications or samples related to the Guide.

Understanding Roles & Permissions

Updated 8 October 2026

experience — not included in the PDF

What RBAC Does

Role-Based Access Control (RBAC) in GCXONE gives administrators granular control over what users can do and which entities they can see.

Key Distinction — Entity Access vs. Privileges: Entity access and privileges are separate concepts in GCXONE. Privileges (configured in the role) determine WHAT actions a user can perform. Entity access determines WHICH customers, sites, devices, and sensors they can see. User-level customization is done through entity access only — there are no user-level privilege overrides.

Why It Matters

- "I have to jump between multiple pages to see what access a role actually grants"
- "Creating a new role takes forever with too many configuration steps"
- "I can't quickly tell what permissions my users have"
- "Two users in the same role need access to different customers, but I have to create separate roles for each"

How It Works

A role is the core unit of access control in GCXONE. Each role combines three elements:

Note: This page covers the GCXONE Role, configured under Settings → Roles. Users also have a separate Genesis Role, assigned when they're invited or edited — see [User Management](#).

Role Information & Users: Basic role details (name and description) and the users assigned to this role.

Module Privileges: Which platform modules users can access, and which specific capabilities are enabled within each. Privileges determine WHAT a user can do.

Entity Assignments: Which customers, sites, devices, and sensors users can access. Entity access determines WHERE a user can operate. Entity assignments can be configured at two levels:

- **Role-Level Entities:** Entities assigned within the role itself, shared by all users in the role
- **User-Level Entities:** Entities assigned to individual users through Edit Entity Access, allowing different users in the same role to access different customers or sites

Tip — Reuse One Role Across Users: Previously, if two users needed the same privileges (e.g., Admin access) but managed different customers, you had to create two separate roles. Now, create one role and customize entity access per user through Edit Entity Access.

Entity Hierarchy

GCXONE organizes entities in a hierarchical structure. The Service Provider is the top-level account (your tenant), and all entities are nested beneath it: Service Provider → Customer → Site → Tower / Device → Sensor (Camera).

Cascading selection: Selecting a customer automatically includes all sites, devices, and sensors beneath it. This ensures new entities are automatically included when using the Include Children toggle and simplifies configuration.

Permission Resolution : When a user has multiple roles (direct assignments + group memberships), all privileges combine additively. Changes take effect within 5 seconds across web and mobile platforms.

Key Capabilities

Default Roles

GCXONE ships with five pre-configured default roles — Super Admin, Admin, Operator, Installer, and End User — each scoped to a typical job function, from full administrative control down to read-only access. Entity access can still be customized per user regardless of which default role they hold, and you can use these roles as-is, customize them, or create new roles from scratch. For exactly which modules and capabilities each default role grants, refer to [Managing Roles & Permissions](#).

Module Privileges

Privileges are organized by platform module, grouped into three categories - Core, Feature, and System. Most modules have a View Page toggle plus one or more capability dropdowns; the dropdowns are locked until View Page is enabled. Privileges determine WHAT actions a user can perform across the platform.

Core:

- Configuration — View Page toggle, plus capability dropdowns for Service Provider, Customers, Customer Groups, Sites, Devices, Sensors (Cameras), Mobile Towers, Audits Management, Alarm Management System, IO Configuration, Audio Management, Analytics, and Configuration Dashboards
- Camera Actions & Alarm Handling — Video Functions, Audio Functions, Camera Controls, Alarm Functions, Isolate time options, and a Stream Time Out (seconds) field

Feature:

- Dashboard — View Page toggle, Main Dashboard capabilities
- HealthCheck — View Page toggle, HealthCheck and Reports capabilities
- ZenMode — Capabilities to access ZenMode from Video Activity Search and from Video Viewer

- Video Activity Search — View Page toggle, Video Activity Search Module and Video Activity Search Capability dropdowns
- Talos — Talos Modules dropdown
- Map — View Page toggle, Map Module, Manage Map Items, and View Map Items dropdowns
- Video Viewer — View Page toggle, Video Tags, Tag Folders, Video Views, and Event Salvo dropdowns
- Marketplace — View Page toggle, Marketplace Module dropdown

System:

- Settings — User Profile, Roles & Permissions, User Management, Reports, Tag Management, Mobile Configure, and Entity Groups capabilities
- Genie (AI Assistant) — Genie AI Assistant capabilities

Each module has a Select All / Remove All option for quick bulk configuration, plus (on most modules) a View Page toggle that enables or disables the entire module.

Entity Access: Three Modes

When configuring entity access during role creation (or editing), three modes are available. Entity access determines WHERE a user can operate - it controls which customers, sites, devices, and sensors are visible and accessible to the user.

- No Entity Access — Users have no entity access by default. Must be assigned per user via Edit Entity Access. Best for: Shared role with individual entity assignments.
- Selected Entities — Users are restricted to the specifically selected entities (with or without children). Best for: Specific sub-lists or tenants with identical access.
- Full Access — Users default to full access for all Customers, Sites, Towers, Devices, and Cameras. Best for: Admin or super-user roles needing unrestricted access.

Regardless of Mode: You can always customize the entity list for specific users through Edit Entity Access, overriding or extending the role-level assignments while keeping their role privileges intact.

The Include Children Toggle: When selecting entities in the tree view, each entity has an Include Children toggle (shown as a blue slider next to the entity name). This toggle has a critical impact on how access works:

Without Include Children: Only the manually selected entities are included. If you select Site A and its 5 devices and 30 sensors individually, the user gets access to exactly those items. Future devices or sensors added under that site will NOT be included automatically - you would need to manually go back to Edit Entity Access and select the new device.

With Include Children: You only need to select the parent entity (e.g., Site A). All devices and sensors underneath are automatically included. Any future devices or sensors added under that site are automatically included - no manual updates needed.

Tip — Default to Include Children: Use Include Children whenever possible. It saves time and ensures new devices are automatically accessible to the right users. Only use manual selection when you specifically need to restrict access to a fixed set of entities.

Edit Entity Access (Per-User Entity Management)

Because privileges always come from the role, per-user customization only ever applies to entity access, never to what a user can do. GCXONE supports this through two modes:

Override Mode: The user's custom entity selection REPLACES the role-level defaults entirely. Use this when you want complete control over a specific user's entity access.

Merge Mode: The selected entities are ADDED on top of the role's existing entity assignments. The user gets both the role-level entities AND the additional user-level entities. Use this to extend a user's access beyond what the role provides.

This is what makes the "one role, many customers" pattern possible (see Example 1 under Best Practices below) — two users can share identical privileges while each sees only their own customers. For the click-by-click steps and screenshots, refer to [Managing Roles & Permissions](#).

Managing Entity Groups

Navigation: Settings → Entity Groups

Entity Groups are saved, reusable collections of entities (customers, sites, devices, and sensors) that act as templates. Instead of manually selecting the same entities every time you configure a role or assign user access, you define the group once and apply it wherever needed. Think of an Entity Group as a named shortcut for a specific set of entities.

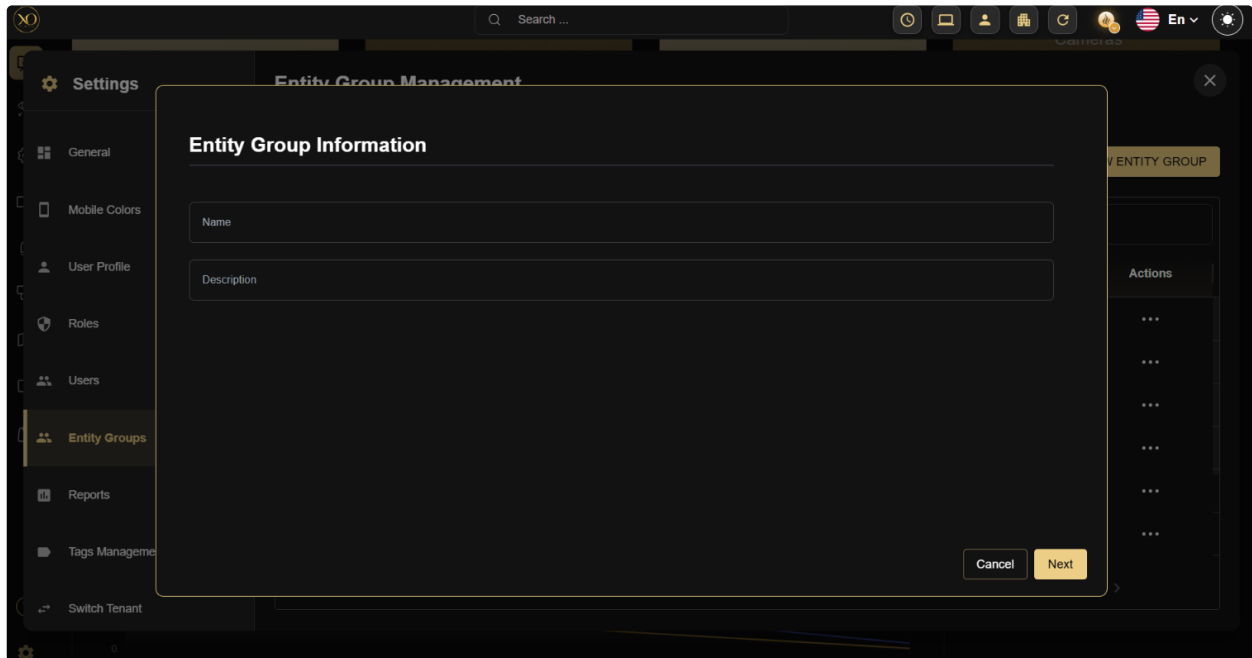
Entity Groups: Define the group once, then select it by name when assigning entity access to any role or user. Any role or user assigned that group automatically gets the correct entities.

The Entity Groups page lists all existing groups in a table showing Name, Description, Entities Count, Roles Count, and Users Count. From here you can search, export, and configure new groups using the Configure New Entity Group button.

Creating an Entity Group

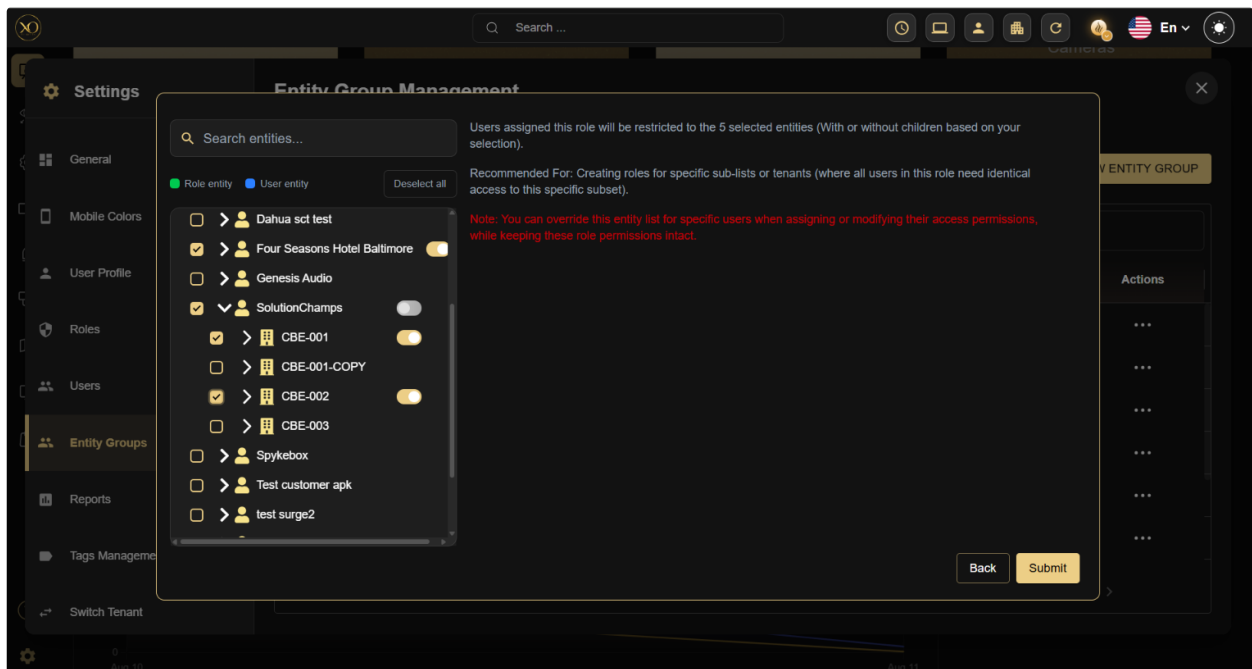
Click Configure New Entity Group to open the two-step creation wizard.

Step 1 - Group Information: Enter a Name and an optional Description for the group, then click Next.



Step 1 of the Entity Group creation wizard, with Name and Description fields for the new group.

Step 2 - Select Entities: Use the entity tree to check the customers, sites, devices, or sensors to include in this group. Use the Include Children toggle next to any entity to automatically include all current and future sub-entities beneath it. A summary on the right shows how many entities are selected and which roles and users are currently affected. Click Submit to save the group.



Step 2 of the Entity Group creation wizard, showing the entity tree with checkboxes and Include Children toggles to select which entities belong to the group.

Assigning an Entity Group to a Role or User

Entity Groups can be applied in two places:

- During role entity assignment (Step 4 of role creation/editing): In the entity selection screen, use the Select Entity Group dropdown to apply a saved group. All entities in that group are immediately loaded into the selection. All users of the role will inherit those entities.
- In Edit Entity Access (per-user): After selecting a user in the Edit Entity Access panel, use the Select Entity Group dropdown at the top to quickly load a group's entities for that user. The Override or Merge mode setting still applies - the group simply pre-populates the entity selection.

Tip — Reuse Entity Groups: Entity Groups are especially useful when multiple roles or users need access to the same set of sites or customers. Create the group once, then apply it across as many roles and users as needed. If the entity list ever changes, update the group in one place and all assigned roles and users automatically reflect the change.

Editing a Role

Navigation: Settings → Roles → [Role Name] → Actions menu ("...")

Editing an existing role is split into two separate actions from the Actions menu: Edit Role Permissions opens the same configuration screen as role creation (Role Information, Users, Module Privileges) without the Entity Assignment step; Edit Role Entities opens the same entity-assignment interface used in Edit Entity Access, scoped to this role. Changes affect all users with this role immediately.

⚠ Warning — Role Changes Apply Immediately: Removing module access or entities may disrupt user workflows. Verify who has this role before making significant changes.

Deleting a Role

Navigation: Settings → Roles → [Role Name] → Delete (via Actions menu)

Clicking Delete opens a confirmation dialog warning that the action cannot be undone. The dialog does not list which users are currently assigned to the role, so check the Users Assigned count on the Role Management page before deleting.

Best Practices

Example 1: Two Regional Admins, One Role

Scenario: You have two regional admins who need identical privileges (full monitoring, alarm control, video export) but Admin A manages Northeast customers while Admin B manages Southeast customers. Previously, this required two separate roles. Now you need just one.

Step 1 - Create the role with no default entity access:

1. Go to Settings → Roles → Configure New Role
2. Role Information: Name = "Regional Admin", Description = "Full monitoring and alarm control for assigned region"
3. Users: Select both Admin A and Admin B from the user grid
4. Module Privileges: Enable Dashboard, Video Viewer, Camera Actions & Alarm Handling, Map with desired capabilities
5. Entity Assignment: Leave "Full access for all entities" OFF and do NOT select any entities. Click Submit.

Step 2 - Assign entity access per user:

- Go to Settings → Roles → Edit Entity Access
- Select Admin A → Choose Merge → Check all Northeast customers (with Include Children enabled) → Submit
- Select Admin B → Choose Merge → Check all Southeast customers (with Include Children enabled) → Submit

Result: Both admins share the exact same role and privileges, but Admin A only sees Northeast customers while Admin B only sees Southeast customers. One role instead of two. When new sites or devices are added under their assigned customers, they're automatically included thanks to Include Children.

Example 2: View-Only Operator

Scenario: Operators who should only view cameras during their shift - no video export, no alarm control, just live viewing and playback for specific sites.

Configuration:

- Settings → Roles → Configure New Role
- Role Information: Name = "View-Only Operator"
- Users: Select the operators who need this role
- Module Privileges: Enable only Dashboard (view only) and Video Viewer (with Live View and Playback).
Leave all other modules disabled.
- Entity Assignment: Select specific sites these operators cover in the entity tree with Include Children enabled

Operators can watch cameras but cannot export footage, access configuration, or control alarms. Perfect for entry-level staff or third-party monitoring services.

Example 3: Installer with Site-Specific Access

Scenario: A field installer needs access to a specific customer site to manage devices and configure sensors. They should only see the entities relevant to their current assignment.

Configuration:

- Create role "Installer" (or use the default Installer role)

- Module Privileges: Enable Configuration (devices, sensors, network settings), Video Viewer (Live View for testing)
- Entity Assignment: No default entity access
- Edit Entity Access: Select the installer user → Merge → Select only the specific site they're working on with Include Children enabled

The installer can only see and manage the specific site and all its devices/sensors. When a new device is installed at that site, it's automatically accessible. When the job is done, remove their entity access or reassign to the next site.

Example 4: Mobile App Access for Field Technicians

Scenario: Field technicians need mobile app access to sites they service, with camera viewing and alarm control.

Configuration:

- Create role "Field Technician" via the role wizard
- Module Privileges: Enable Video Viewer (Live View), Camera Actions & Alarm Handling (Arm/Disarm), Map (Live Stream View)
- Entity Assignment: No default entity access. Use Edit Entity Access to assign each technician their service area with Include Children enabled.

Mobile App Behavior: The technician logs into the GCXONE mobile app and sees only their individually assigned sites. They can view live cameras and arm/disarm from their phone. Permission changes apply to mobile within 5 seconds. No need to manage mobile permissions separately or create individual roles.

Related Resources

- For a step-by-step admin walkthrough with troubleshooting, refer to [Managing Roles & Permissions](#)

- For the full catalog of every individual permission, refer to [Privileges](#)
- For understanding the entity hierarchy, refer to [Organization & Hierarchy Setup](#)
- For managing users, refer to [User Management](#)
- For understanding audit logs, refer to [Audit](#)
- For contacting support, refer to [Contact Support](#)